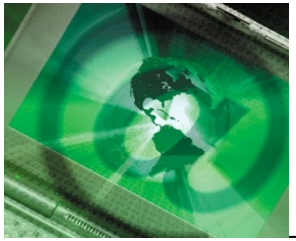
U.S. Department of Agriculture

Office of the Chief Information Officer

USDA Rules of Behavior User Training

Next

AgLearn Course



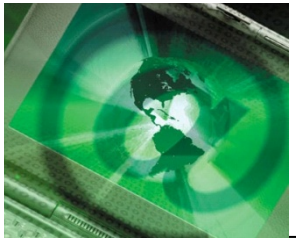
USDA Rules of Behavior

USDA is required by law to ensure that anyone who utilizes USDA Information Technology (IT) resources is aware of his or her responsibilities and complies with these Rules of Behavior.

Public Law 107-347 dated December 17, 2002; the E-Government Act of 2002; and Office of Management and Budget (OMB) Circular A-130, Appendix III require protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

Previous

Next



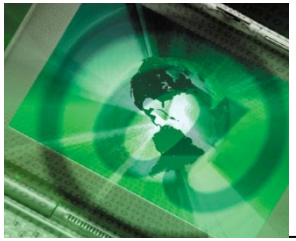
USDA Rules of Behavior

These Rules of Behavior establish expected and acceptable computing behaviors.

Because written guidance cannot cover every contingency, users are also required to use sound judgment and the highest ethical standards in their decision making.

Previous

Next



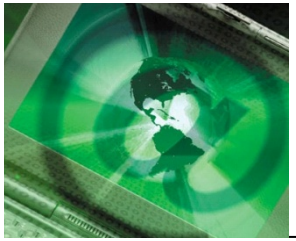
USDA Rules of Behavior

USDA will take corrective action and/or enforce the use of penalties against any user who violates any USDA or Federal system security policy, using any and/or all of the following:

- Corrective actions (taken in accordance with existing rules, regulations, and laws) include:
  - Written reprimands;
  - Temporary suspension from duty;
  - Reassignment or demotion; and
  - Termination of Federal employment
- Suspension of system privileges.
- Possible criminal prosecution.

Previous

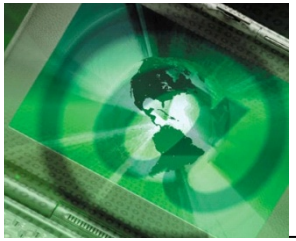
Next



USDA Rules of Behavior

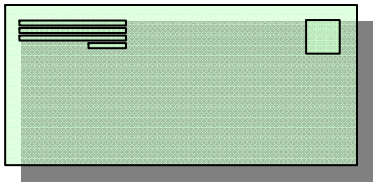
The following nonofficial activities are prohibited on any government owned or leased computer:

- Gambling.
- Intentionally visiting and downloading material from pornographic Web sites.
- Lobbying Congress or any government agency.
- Campaigning – political activity.
- Any type of continuous audio or video streaming from commercial, private, news, or financial organizations, except as expressly authorized by management.
- Activities that are connected with any type of outside employment.
- Endorsement of any non-government products, services, or organizations.



USDA Rules of Behavior

Email

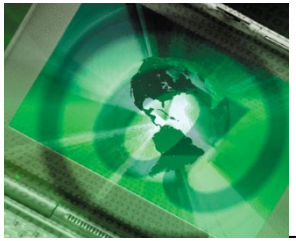


The following apply regarding email activity:

- Automatic filters will be in place to help prevent inappropriate and offensive messages from passing through USDA email gateways.
- Any email on a government email system is the property of the government and may become an official record.
- The use of IT resources constitutes consent to possible monitoring and security testing. User's consent to monitoring and security testing ensures proper security procedures and appropriate usage are being observed for USDA IT resources.
- Monitoring of email and other IT resources by management will be done only in accordance with established USDA policy and guidelines.
- Users are prohibited from using USDA IT resources to send, receive, retain, or proliferate any messages or material that is fraudulent, inappropriate, offensive, harassing, or is of a sexual nature.

Previous

Next

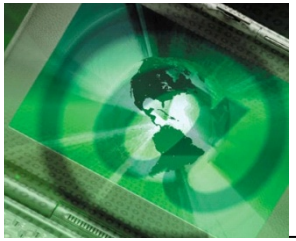


USDA Rules of Behavior

Access

Users shall access and use only information for which they have official authorization. Users shall:

- Follow established procedures for accessing information, including use of user identification, user authentication, passwords, and other physical and logical safeguards.
- Follow established channels for requesting and disseminating information.
- Access only those files, directories, and applications for which access authorization by the system administrator has been granted.
- Use government equipment only for approved purposes.



USDA Rules of Behavior

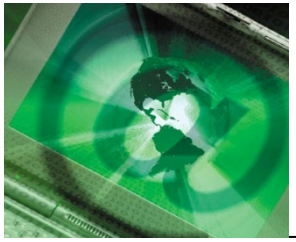
Access *(continued)*

In addition, users shall NOT:

- Give information to other employees or outside individuals who do not have access authority.
- Store sensitive or confidential information on a system unless access control safeguards (e.g., passwords, locked rooms, and protected local area network (LAN) storage areas) are used.
- Use their trusted position and access rights to exploit system controls or access data for any reason other than in the performance of official duties.
- Browse files (i.e., what can be accessed).

Previous

Next

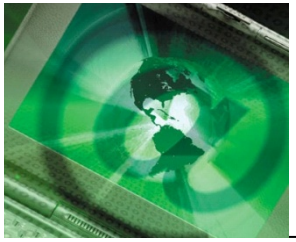


USDA Rules of Behavior

Accountability

Users are accountable for actions related to information resources entrusted to them. Users shall:

- Behave in an ethically, technically proficient, informed, and trustworthy manner when using systems.
- Be alert to threats and vulnerabilities such as malicious programs and viruses.
- Participate in IT security training and awareness programs.
- Not install or use unauthorized software on USDA equipment.
- Comply with all software licensing agreements, and not violate Federal copyright laws.
- Know that there may be monitoring and that there is no expectation of privacy on USDA IT resources.

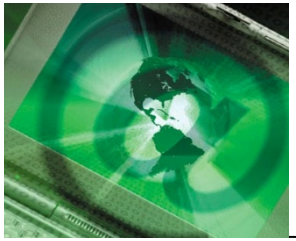


USDA Rules of Behavior

Accountability *(continued)*

In addition, users shall:

- Prevent others from using their accounts by:
  - Logging out or locking the screen when leaving the vicinity of their terminals or PCs.
  - Setting a password on automatic screen savers.
  - Helping to remedy security breaches, regardless of who is at fault.
  - Immediately notifying the system administrator whenever there is a change in role, assignment, or employment status and/or when access to the system is no longer required.
- Practice good citizenship when accessing external systems by complying with that system's rules of behavior.
- Read and understand banner pages and end user licensing agreements.

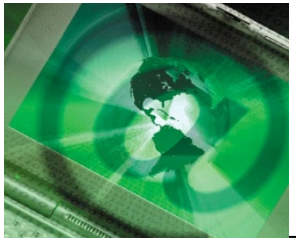


USDA Rules of Behavior

Confidentiality

Access to confidential or sensitive information must be restricted to authorized individuals who need it to perform their jobs. This entails refraining from intentional disclosure and using measures to guard against accidental disclosure. Users shall:

- Protect confidential or sensitive information by using encryption, and limiting the collection, disclosure, sharing and use of PII data. Never access or disclose personal information or other sensitive data unless it is necessary to perform official duties.
- Not send highly sensitive information via email, unless it is encrypted.
- Ensure that sensitive information sent to a fax or printer is handled in a secure manner (e.g., use of a cover sheet that contains a statement that the faxed information is confidential).



USDA Rules of Behavior

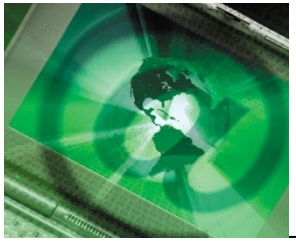
Confidentiality *(continued)*

In addition, users shall:

- Not store or transmit confidential information on public access systems, such as email or the Internet.
- Lock up media, such as paper copies, tapes, and disks containing confidentially sensitive data. Dispose of media according to approved procedures.
- Never access someone else's account or files without a supervisor's formal authorization.
- To the extent possible, ensure that computer monitors are located in such a way as to eliminate viewing by unauthorized persons.

Previous

Next

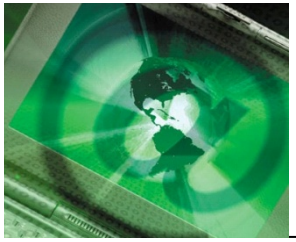


USDA Rules of Behavior

Confidentiality *(continued)*

Users shall also:

- Lock workstations when away from the desk as a preventative measure to ensure that unauthorized individuals cannot read, copy, alter, or steal printed or electronic information.
- When requesting that another individual receive, pick up or deliver application systems input and output information and media, ensure that the individual is authorized.
- Ensure that confidential or sensitive data are properly erased when disposing of hardware or media.

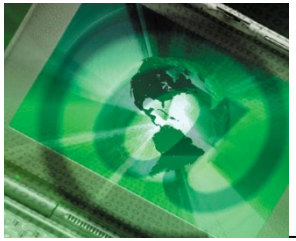


USDA Rules of Behavior

Integrity

Users must protect the integrity and quality of information. This includes, but is not limited to:

- Reviewing quality of information as it is collected, generated, and used to ensure that it is accurate, complete, and up to date.
- Taking appropriate training before using a system to learn how to correctly enter and change data.
- Protecting information against viruses and similar malicious code by:
  - Using virus detection and correction software.
  - Avoiding unofficial software, such as shareware and public domain software.
  - Discontinuing use of a system at the first sign of virus infection.
- Never knowingly entering unauthorized, inaccurate, or false information into a system.

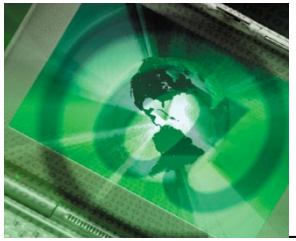


USDA Rules of Behavior

Availability

Computer systems and media must be protected from environmental hazards such as fire, water, heat, and food spills. They must also be protected from theft, unauthorized alteration, and careless handling. Users shall:

- Use physical and logical protective measures such as the following to prevent loss of availability of information and systems.
  - Ensure that there are backups of information for which they are responsible.
  - Protect systems and media where information is stored.
  - Store media in protective jackets.
- Keep media away from devices that produce magnetic fields (such as phones, radios, and magnets).
- Follow contingency plans.

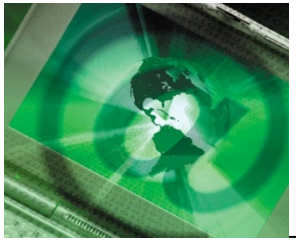


USDA Rules of Behavior

Passwords and User IDs

Users are responsible and accountable for any actions taken under their user ID. Users shall:

- Protect passwords from access by other individuals.
- Never give a password to another person, including a supervisor or a computer support person.
- Not ask anyone for their password.
- Construct effective passwords by following USDA password policy for complex passwords.

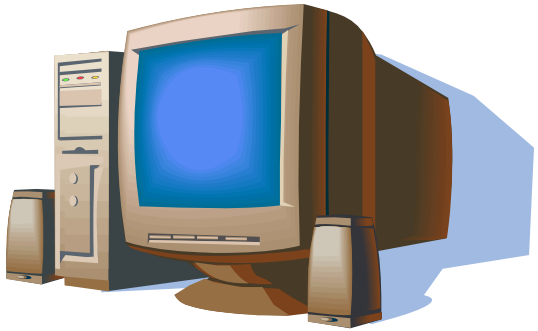


USDA Rules of Behavior

Hardware

Users must protect computer equipment from damage, abuse, theft, and unauthorized use. Users shall:

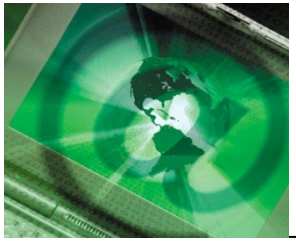
- Protect computer equipment from hazards such as:
  - Extreme temperatures;
  - Electrical storms;
  - Water and fire;
  - Static electricity;
  - Spills from food and drink;
  - Dropped objects;
  - Excessive dusty environments; and
  - Combustible materials.



- Keep an inventory of all equipment assigned to them.
- Only use equipment for which they have been granted authorization.

Previous

Next

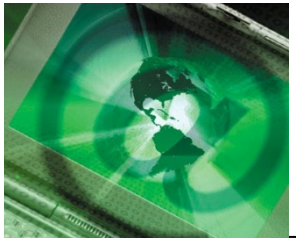


USDA Rules of Behavior

Hardware *(continued)*

In addition, users shall:

- Not leave computer equipment in a parked car or in an unsecured location where it might be stolen.
- Follow established procedures when removing equipment from USDA premises. This usually requires a property pass.
- Not install or use unauthorized software or hardware on the network, including personal laptop computers, pocket computers, or personal digital assistants and network enabled cellular phones, except as expressly authorized.
- Not alter the configuration, including installing software or peripherals, on government equipment unless authorized.
- Notify management before relocating computing resources.
- When possible, use physical locking devices for laptop computers and use special care for other portable devices.

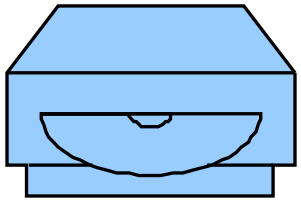


USDA Rules of Behavior

Software

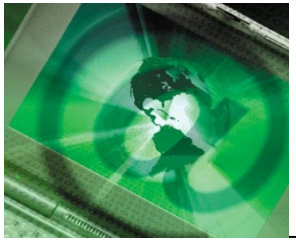
Do not install non-authorized, standard, public domain, or shareware software on your computer without approval from the appropriate management official. Computer users must protect USDA owned software and equipment from malicious software. Users shall NOT:

- Use USDA purchased software on personally owned or non-USDA computers unless authorized.
- Alter the configuration, including installing software or peripherals, on government computer equipment unless authorized.



Previous

Next

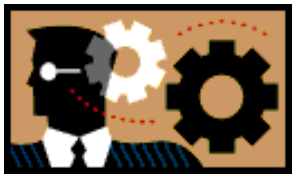


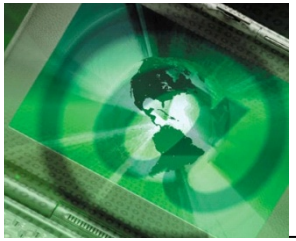
USDA Rules of Behavior

Software *(continued)*

In addition, users shall:

- Comply with all software licensing agreements and Federal copyright laws.
- Not download, install, or run security programs or utilities that might reveal weaknesses in the security measures or access privileges of any system unless otherwise expressly authorized."

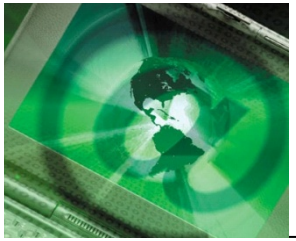




USDA Rules of Behavior

Awareness

Annual IT Security Awareness and Privacy Training are mandatory for all USDA employees and contractors. New employees, contractors, partners, and volunteers are required to complete the awareness training prior to gaining access to systems. All users must stay abreast of security policies, requirements, and issues. Users must make a conscientious effort to avert security breaches by staying alert to network vulnerabilities.



USDA Rules of Behavior

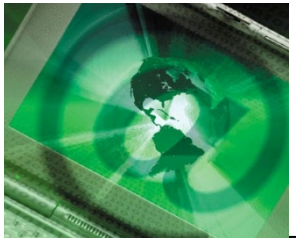
Incident Reporting

Each user is responsible for reporting any form of security violation, whether waste, fraud, or abuse through the USDA incident reporting mechanism. Users shall:

- Report security incidents, or any incidents of suspected fraud, waste, or misuse of USDA resources to the USDA Help Desk (1-888-926-2373 or USDA PII Hotline at 1-877-PII-2-YOU) or to the appropriate agency IT Information Security Manager.
- Report security vulnerabilities and violations as quickly as possible to the USDA Help Desk (1-888-926-2373 or USDA PII Hotline at 1-877-PII-2-YOU) or to the appropriate agency IT Information Security Manager so that corrective action can be taken.
- Take reasonable action immediately upon discovering a violation to prevent additional damage, such as logging out a terminal or locking up property.
- Cooperate willingly with official action plans for dealing with security violations.

Previous

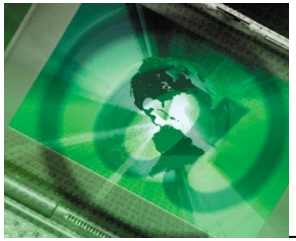
Next



USDA Rules of Behavior

Prohibition of the Use of Wireless Networks

All USDA employees and contractors are prohibited from using any unauthorized 802.11xx network devices within USDA buildings. Users must ensure that any wireless capable devices in their control, including laptops, PDAs, and Bluetooth telephones have their wireless networking disabled. The only acceptable use of wireless communications is through the USDA provided messaging service.



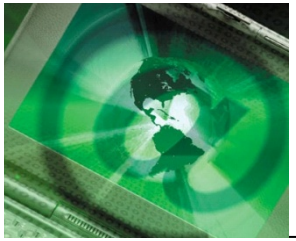
USDA Rules of Behavior

Prohibition of Peer-to-Peer File Sharing

Users are prohibited from using Peer-to-peer (P2P) file sharing. P2P file sharing poses a threat to IT security. It allows employees to transfer files between computers without proper security controls. These programs can be used to distribute inappropriate materials, violate copyright law and put government information at risk.

Previous

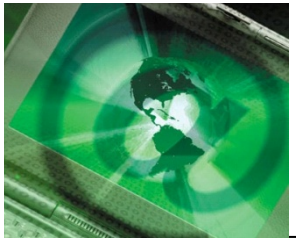
Next



USDA Rules of Behavior

There are no exceptions to the requirement that all employees, contractors, partners, and volunteers comply with these rules of behavior. If you are not sure whether your intended computer use is prohibited, you should NOT do it. Consult with your supervisor or appropriate management official for clarification.

USDA requires employees, contractors and partners to acknowledge that they understand their responsibilities and accountability for using USDA information and resources. The completion of this training constitutes the acknowledgment of these USDA Rules of Behavior.



USDA Rules of Behavior

USDA

SURVEY - USDA Confirmation Survey

1. This confirms that I successfully completed the training.
☐ I have read and understand the Rules of Behavior.

Per Departmental Regulation 3620- 001, AgLearn is the official training system for USDA, and the source of all data for audits, mandatory training completions, and records examinations relating to personnel actions. All data contained in AgLearn is subject to examination by the USDA Inspector General and/or the Office of Personnel Management without notice at any time. False claims of completed training submitted by employees using AgLearn as recorded in their Learning History file, if substantiated, may be used to support disciplinary or other administrative action.

Submit

EXIT